EVERYDAY CYBERSECURITY
Identify & Protect Yourself Against
25 Common Cyber Frauds
CLAIM PRIZE
@CYBER24X7

Contents

Chapter 1: The "Fear & Authority" Traps 4

Threat #1: The "Digital Arrest" / Police Impersonation Scam 4

Threat #2: The Fake Courier / Customs Parcel Scam 5

Threat #3: Utility Bill Disconnect Scam (The Light-Out Threat) 6

Threat #4: KYC Expiry / Bank Account Update Fraud 7

Threat #5: Income Tax Refund Scam 7

Chapter 2: Your Money & Banking (Financial Fraud) 9

Threat #6: The QR Code Scam (The "Scan to Receive" Lie) 9

Threat #7: The "Wrong Number" / Accidental Transfer Scam 10

Threat #8: Credit Card Reward Points Scam 10

Threat #9: ATM Skimming & Shoulder Surfing 11

Threat #10: Fake Loan Apps (The Extortion Trap) 13

Chapter 3: Mobile & Communication (The Device Hijack) 14

Threat #11: SIM Swap Fraud (The Number Takeover) 14

Threat #12: The "Customer Service" Imposter Call 15

Threat #13: The Malicious Text Message (Smishing) 16

Threat #14: WhatsApp "Lost Phone" Scam 16

Threat #15: Wi-Fi Spoofing – Free Unlimited Internet Scam 17

Chapter 4: The Emotional Manipulators (Heart & Greed) 19

Threat #16: Romance Scams (The "Military Doctor" Trap) 19

Threat #17: The "Grandchild in Trouble" (AI Voice Scam) 20

Threat #18: Sextortion (The Video Call Blackmail) 20

Threat #19: Part-time Job / "Task" Scams 21

Threat #20: Lottery & Inheritance Scams 22

Chapter 5: Technical Hygiene & Future Threats 23

Threat #21: Deepfakes (AI Video/Audio) - The Technical View 23

Threat #22: Juice Jacking 24

Threat #23: Weak Passwords & Reuse 24

Threat #24: Social Media Cloning 25

Threat #25: Malicious Email Attachments – No. 1 Attack Vector 26

Introduction

Welcome to your guide to staying safe in the digital world.

If you are a senior citizen, a hardworking housewife, or a small shop owner , you are likely the most frequent target of digital criminals. Why? Because somewhere on the internet – your information related to your phone number, email id etc. has been leaked and hackers know your identity and you have money.

This book is built on one simple idea: **You do not need to be a technology expert to be cyber secure.**

We will explain 25 common threats in plain language, using real-world scenarios like UPI payments, courier tracking, and electricity bills. This knowledge will be your shield. By understanding the criminal's tricks, you instantly take away their power , you stop them in their tracks.

So Let's Go Ahead!

Chapter 1: The "Fear & Authority" Traps

"The most effective scam is one that makes you forget logic and only feel panic."

This chapter focuses on scams where the criminal pretends to be someone powerful—a police officer, a government official, or a reputable courier company. They use fear and urgency to bypass your common sense.

Threat #1: The "Digital Arrest" / Police Impersonation Scam

The highest-loss scam currently targeting unsuspecting users and retired citizens.

- **Targets:** Affluent, retired citizens, business owners.
- **Medium of Attack:** VoIP Call / WhatsApp Video Call, sometimes from International numbers
- **Objective:** To terrify the victim into transferring their entire savings into a "safe account" (which is the scammer's account).

The Scenario:

You receive a VoIP call. The person claims to be from the Customs Department or CBI. They say: "We intercepted a suspicious package/parcel with your Aadhaar number. It contains illegal drugs/SIM cards. You are linked to money laundering. You must join a video conference with the Police/Judge immediately."

On the video call, actors in police uniform threaten you with "Digital Arrest." They demand you empty your bank accounts into a "temporary, protected RBI account" for verification. For authenticity, they even have banners in the background as if they are calling you from a Police Office or Court.

Check this link : https://economictimes.indiatimes.com/news/new-updates/viral-video-scammer-posing-as-mumbai-police-calls-real-cop-by-mistake-gets-a-shocking-surprise-on-zoom/articleshow/115356729.cms

Fake Cop on WhatsApp call

Phase	Details
Steps to Identify	1. **The Setup:** Real law enforcement does not use WhatsApp video calls or Skype for official arrests. 2. **The Money Demand:** Police/CBI will never ask you to transfer money to a "safe account" to prove your innocence. Fines are paid in court, not via UPI. 3. **Secrecy:** They order you to stay on the phone and not talk to family or lawyers. Isolation is the core of the trick.
Steps to Remediate	1. **Hang Up:** Cut the call immediately. 2. **Verify Offline:** Call your nearest police station or a lawyer you trust. They will confirm the entire story is fake. 3. **Block:** Block the number and inform your family.
Remember	**Rule:** If you are accused of a crime, the Police **will come to your door**. They will not conduct an "arrest" via a video call.
Reporting	**Whom:** Cyber Crime Helpline **1930** immediately and your Phone Service Provider.

Threat #2: The Fake Courier / Customs Parcel Scam

The sibling of the Digital Arrest scam, starting with a lesser threat.

- **Targets:** People who frequently shop online or receive international packages.
- **Medium of Attack:** Phone Call / SMS.
- **Objective:** To get remote access to your device or initiate the Digital Arrest scam (Threat #1).

The Scenario:

You receive a call claiming to be from FedEx/DHL/Blue Dart. They state: "Your international parcel is held up at Customs because it contains prohibited items (e.g., unauthorized currency, illegal books). You must pay the fine immediately or face legal action." They then transfer the call to a "Customs Officer" who escalates the threat, demanding your bank details or asking you to install a remote access application or software on your phone or laptop. The application or software may have RBI logo or some Government office logo to win your trust, however this software once installed will take complete control of your laptop or mobile to read your OTP , passwords etc.

Phase	Details
Steps to Identify	1. **The Transfer:** The fact that a "courier executive" can instantly transfer you to an "officer" shows it is a coordinated criminal gang. 2. **The Remote App:** The immediate demand to download an app like **AnyDesk** or **TeamViewer** (which gives them full control of your phone). **This is the biggest red flag.** 3. **The Unsolicited Call:** If you aren't expecting a package, the call is definitely fake. If you are, verify the tracking number on the **official** website not on the website being provided by the scammer.

Steps to Remediate	1. **Do Not Install:** Never install AnyDesk, TeamViewer, or QuickSupport on your phone for a stranger. 2. **Official Verification:** Cut the call. Go to the courier's official global website (e.g., FedEx.com), enter your tracking number, and check the status.
Remember	**Rule:** If the Customs Department has an issue, they send an official, written notice to your address, not a frantic call asking for money via UPI.
Reporting	**Whom:** Cyber Crime Helpline **1930** immediately.

Threat #3: Utility Bill Disconnect Scam (The Light-Out Threat)

A common scam that exploits the urgency of losing essential services.

- **Targets:** People who pay bills online, senior citizens, users who keep following or joining unknown groups on WhatsApp, Telegram etc.
- **Medium of Attack:** SMS or WhatsApp message and sometimes call also.
- **Objective:** To steal money via UPI or gain remote access to the phone.

The Scenario:

An SMS reads: "Urgent! Your electricity/gas will be disconnected tonight due to unpaid bill. Call this number immediately to avoid cut-off." Mostly these messages are sent on last working day of week or on a holiday to give little chance to user to contact the government official number.

Phase	Details
Steps to Identify	1. **The Urgency:** The message threatens immediate disconnection (e.g., "Tonight at 10 PM"). Utility companies give weeks of notice. 2. **The Number:** The message asks you to call a normal 10-digit mobile number, not an official utility company helpline. 3. **The Link/APK:** They ask you to click a malicious link or install a remote control app (AnyDesk/TeamViewer) to "pay the small pending amount." Or they provide a fake look-alike “mseb.eb1ll.net” or electricbill.pay-now-mseb.org” links or QR codes for payment.
Steps to Remediate	1. **Ignore the Message:** Delete the message immediately. 2. **Official App:** Go to your **official** electricity/gas company website or app and check your outstanding balance there. Don't trust the text message. 3. **No Remote Control:** Never install AnyDesk or grant remote access to your device to an unknown caller.
Remember	**Rule:** If you think your bill is overdue, check your **official** bill copy or app. Never pay through a random UPI number or an online site given over the phone or SMS.
Reporting	**Whom:** Your Utility Provider's Official Helpline & Cyber Crime (1930).

Threat #4: KYC Expiry / Bank Account Update Fraud

Exploiting the fear of losing access to your money.

- **Targets:** Bank customers, mobile wallet users (Paytm/Airtel money/GPay or UPI applications).
- **Medium of Attack:** Phone Call (Vishing) or SMS (Smishing).
- **Objective:** To steal your bank credentials, OTP, or remote control access.

The Scenario:

A call from someone claiming to be from "HDFC/SBI KYC Department." They say, "Your account will be frozen in 2 hours because your KYC documents have expired. To prevent this, share the OTP we are sending you now." The callers are very pleasant speaking and many a times have your correct name and part of your account number.

Phase	Details
Steps to Identify	1. **The OTP Request:** Banks and KYC departments never call and ask you to share the OTP/PIN/Password. 2. **The Urgency:** They create extreme panic—"frozen account," "expired card"—to prevent you from thinking clearly. 3. **The Spoofed Number:** Their caller ID might *look* like your bank, but banks use official, recorded lines and rarely call to demand KYC details over the phone.
Steps to Remediate	1. **Hang Up:** Immediately cut the call. Call your bank's official toll-free number (printed on your card or passbook) or visit the official website of the bank to verify. 2. **Do Not Share:** Never share the OTP, CVV, or PIN with anyone, even if they claim to be from the Reserve Bank of India (RBI). 3. **Official Channel:** IF required, update KYC only by visiting your branch or using the **official** banking app/Net Banking portal. DO NOT OPEN LINKS SENT via SMS/WhatsApp or from unofficial/unknown email ID's.
Remember	**Rule:** OTP means "One Time Password." It's for **you** to use, not for anyone else to "verify."
Reporting	**Whom:** Your Bank's Fraud Department & Cyber Crime (1930).

Threat #5: Income Tax Refund Scam

Targeting your hope for a quick government payment.

- **Targets:** Taxpayers, individuals expecting government payments.
- **Medium of Attack:** Email (Phishing) or SMS.
- **Objective:** To steal your Net Banking ID and Password.

The Scenario:

You receive an email that looks exactly like the Income Tax Department's official mail. It says: "Great News! You are due a refund of ₹45,000. Click this link to confirm your bank account details and receive the payment immediately."

Phase	Details
Steps to Identify	1. **The Link:** The email or SMS contains a link to a **fake website** that looks like the Income Tax portal, but the URL is slightly wrong (e.g., incometax.net or inc0metax.net instead of incometax.gov.in). On mobiles since fonts are small, its very easy to fall prey to such tactic. 2. **Net Banking Details:** The fake site asks for your **Bank Account Number, IFSC Code, and Net Banking Password** to "verify" the transfer. **NO legitimate refund site asks for your Net Banking Password.** 3. **Unexpected:** If you haven't filed IT returns or if the amount seems too high/unexpected, be suspicious. Don't ever visit such sites and don't indulge in any information exchange.
Steps to Remediate	1. **Official Portal Only:** Only check your refund status by logging into the **official** Income Tax portal (URL is www.incometax.gov.in). 2. **Check Sender Address:** Look at the sender's email. Is it a government domain (@gov.in or @nic.in) or a common Gmail/Yahoo account? Tax refund emails are sent only from @gov.in only. 3. **Antivirus Check:** Scan your computer for viruses if you accidentally clicked the link. 4. Do check that your mobile is not installed with any unknown application. 5. **Change Browser Stored Passwords :** In few cases, the hackers stole the passwords stored in the browsers and later used the passwords to take control of the account of the user. Since users store very sensitive information like PAN, Aadhar or Passports, a compromise of the email account lead to identify theft and financial frauds later.
Remember	**Rule:** Government money (refunds, benefits) is deposited automatically. They never need your Net Banking password or OTP to give you money.
Reporting	**Whom:** Email Provider (Mark as Phishing) & Cyber Crime (1930).

Chapter 2: Your Money & Banking (Financial Fraud)

"The modern bank robber doesn't wear a mask or carry a gun. He carries a smartphone and polite language."

In this chapter, we look at the most common ways criminals try to trick you out of your hard-earned money. These scams rely on **confusion** about how banking technology works.

Threat #6: The QR Code Scam (The "Scan to Receive" Lie)

The #1 fraud affecting people selling items online or small shopkeepers.

- **Targets:** People selling old furniture on OLX/Facebook, Small Shopkeepers, Landlords collecting rent.
- **Medium of Attack:** Google Pay, PhonePe, Paytm, WhatsApp.
- **Objective:** To trick you into authorizing a payment *from* your account while you think you are receiving one.

The Scenario:

You are selling an old bed on OLX or other online used products site. A buyer calls immediately, agrees to the price, and says: "I cannot come today, but I will pay you an advance now. I am sending a QR code. Just scan it with your GPay to receive the money instantly." Once scanned , your bank account will be emptied.

Phase	Details
Steps to Identify	1. **The Rule:** In the history of UPI, **you NEVER need to scan a QR code to RECEIVE money.** You only scan to PAY. 2. **The PIN:** The app asks for your 4 or 6-digit UPI PIN. **PIN is only used when money leaves your account.** 3. **The Text:** The screen will say "Paying ₹5,000," but the scammer will say, "No, that is a verification message, ignore it." Do not ignore it.
Steps to Remediate	1. **Stop:** If anyone asks you to scan a code to get money, cut the call. 2. **Read:** Look at the button you are pressing. Does it say **"Pay"** or **"Send"**? If yes, you are losing money. 3. **Share Number Only:** To receive money, you only need to give your Phone Number or your UPI ID, code scanning is not needed.
Remember	• **Scan QR + Enter PIN = Your account is debited - MONEY FLIES OUT.** • **For Receiving Money = Do NOTHING.**
Reporting	**Whom:** Your Bank & The App Support. **How:** If you have transacted and realised the loss of money, Tap the transaction > "Report Dispute/Fraud" immediately. If you report within 2hrs of fraud, recovery chances increase greatly.

Threat #7: The "Wrong Number" / Accidental Transfer Scam

A trap that turns you into a criminal or steals your money.

- **Targets:** UPI users.
- **Medium of Attack:** UPI (GPay/PhonePe/Airtel UPI etc).
- **Objective:** To double-dip (steal twice) or use your account for money laundering.

The Scenario:

Suddenly, you receive ₹5,000 in your bank account. A few minutes later, you get a panicked call: "Sir/Madam, I sent this money to you by mistake. It was for my mother's hospital fees. Please send it back to this other number immediately."

Phase	Details
Steps to Identify	1. **The Request:** They ask you to return the money to a **different** number, not the one it came from. 2. **The Fake SMS:** Sometimes, no money actually came. They just sent a fake SMS that *looks* like a bank credit alert. Always check your actual balance in the app. 3. **The Trap:** If the money *did* come, it might be stolen money. If you send it back manually, and then the original victim complains, the bank will reverse the transaction. You will lose the money *twice*.
Steps to Remediate	1. **Do Not Transact:** Tell the caller: "I will not transfer it back manually. Please visit your bank and file a reversal request." 2. **Let the Bank Handle It:** If it was a genuine mistake, their bank can reverse it officially. Do not become the middleman. 3. **Report:** Inform your bank that you received an unknown sum.
Remember	**Rule:** Never manually refund an "accidental" transfer. Tell them to follow official banking procedures.
Reporting	**Whom:** Your Bank only. **How:** Send an email or visit the branch to declare the unknown transaction.

Threat #8: Credit Card Reward Points Scam

Targeting your greed to expire your bank balance.

- **Targets:** Credit Card holders (especially HDFC/SBI/ICICI/Axis users).
- **Medium of Attack:** SMS / WhatsApp.
- **Objective:** To steal your OTP and empty your credit card limit.

The Scenario:

You get an SMS: "Dear Customer, your Bank Credit Card points worth ₹9,850 will EXPIRE tonight. Click here to convert into cash/gift card: http://somebank-reward-redeem.com"

Phase	Details
Steps to Identify	1. **The Link:** Look at the URL carefully , the hackers send look-alike URL's like yourcard.sbiindia.net or points.hdfcindia.org.in . It is never the official bank website. Fraudster usually add words like "redeem," "bonus," or "points" to a fake look alike domain to fool users. 2. **The Form:** When you click, it asks for your Card Number, Expiry Date, CVV, *and* OTP. A real bank never needs all this just to redeem points. 3. **The Amount:** The reward amount is always surprisingly high (e.g., ₹5,000+) to make you greedy.
Steps to Remediate	1. **Delete:** Delete the SMS. 2. **Official App:** If you really want to check points, open the official Net Banking app on your phone. You will likely see you have only few rupees worth of points, proving the SMS was a lie. 3. **Block Card:** If you entered details, block your card immediately via the app and also call you bank to notify.
Remember	**Rule:** Banks never send links to redeem points. Points are redeemed only inside the official Banking Portal.
Reporting	**Whom:** Forward SMS to **1909**.

Threat #9: ATM Skimming & Shoulder Surfing

The old-school way of stealing money that still works.

- **Targets:** Seniors, people at ATMs.
- **Medium of Attack:** Physical ATM Machine.
- **Objective:** To clone your card and steal your PIN.

The Scenario:

You go to an ATM. You insert your card, type your PIN, and withdraw cash. Two days later, money is withdrawn from your account in a different city.

How? A "Skimmer" (a fake reader) was placed over the card slot to copy your card data, and a tiny hidden camera captured you typing your PIN.

Here is a link to a video : https://www.youtube.com/watch?v=WzX_8mzUIvk

Phase	Details
Steps to Identify	1. **Wobbly Slot:** Before inserting your card, wiggle the card reader slot. If it moves, shakes, or feels like loose plastic, do not use it. 2. **Sticky Keys:** If the keypad feels thick or sticky, it might have a fake overlay. 3. **Shoulder Surfing:** Is someone standing too close behind you? They might be trying to see your PIN.

Steps to Remediate	1. **Cover Hand:** Always cover your typing hand with your other hand or wallet while entering the PIN. Even if they clone your card, they can't use it without the PIN. 2. **Cancel:** If the machine looks suspicious, press Cancel and leave. 3. **Alert:** Tell the security guard. And Call banks support number to inform them as well.
Remember	**Habit:** Wiggle the card slot. Cover the keypad. Never let strangers "help" you inside an ATM.
Reporting	**Whom:** The Bank ATM Guard or Toll-Free Number displayed in the ATM.

Threat #10: Fake Loan Apps (The Extortion Trap)

The most vicious scam causing immense mental harassment.

- **Targets:** People in financial need or people who subscribe to unknown WhatsApp groups or Telegram channels for quick money
- **Medium of Attack:** Android Apps (often from links or Play Store).
- **Objective:** Extortion and blackmail using your private photos/contacts.

The Scenario:

You download an app that promises an "Instant Loan in 5 minutes, No CIBIL check." To get the loan, the app asks for permissions: Contacts, Gallery/Photos, Camera. You get ₹3,000 credited (even if you asked for ₹5,000). Seven days later, they demand ₹10,000 back. If you don't pay, they send morphed (nude) photos of you or your family members to you and threaten that these will be send to all on your contact list if not paid.

Phase	Details
Steps to Identify	1. **Permissions:** A loan app needs your financial data, not your **Gallery** or **Contacts**. If it asks for these, it is a scam. 2. **No Paperwork:** Legitimate banks (NBFCs) always need proper ID verification. "No documents required" is a red flag. 3. **Short Tenure:** RBI rules say minimum loan tenure is usually 90 days. These apps demand money back in 7 days.
Steps to Remediate	1. **Do Not Pay:** Even if you pay, they will demand more. Paying never stops them. 2. **Uninstall:** Remove the app immediately. 3. **Alert Contacts:** Put a WhatsApp status/Social Media post saying: "My phone was hacked. If you receive any strange messages or photos about me, it is a fraud and these are DeepFake photos. Please ignore." **4. Inform Police**: Do inform police , there is no other way could stop them.
Remember	**Rule:** Only take loans from apps listed on the RBI website or official banking apps. Never give "Gallery" permission to a finance app.
Reporting	**Whom:** Cyber Crime Police. **How:** Call **1930** immediately.

Chapter 3: Mobile & Communication (The Device Hijack)

"Your mobile phone is your digital wallet and your digital identity. If the thief steals the wallet, they steal your life."

This chapter focuses on threats that compromise your device itself, primarily through phone calls, text messages, or malicious apps, allowing criminals to take over your bank accounts, WhatsApp, and identity.

Threat #11: SIM Swap Fraud (The Number Takeover)

The most sophisticated way to steal your OTP and access your bank accounts.

- **Targets:** Users who have their information compromised due to various reasons such as hacking of a online grocery platform or data leak from a service provider like courier company etc.
- **Medium of Attack:** theft of documents or email hacking, via physical cloning.
- **Objective:** To get a duplicate SIM card of your number, thereby receiving all your OTPs.

The Scenario:

You suddenly notice your phone stops receiving calls and SMS. Your phone says "No Service" or "SIM Error." In reality, a scammer has already gone to your telecom provider with fake ID proof, convinced them your phone was lost, and gotten a new SIM card for your number. Within minutes, they log into your bank accounts, use the "Forgot Password" feature (receiving the OTP on their new SIM), and drain your account.

Phase	Details
Steps to Identify	1. **Loss of Service:** If your phone loses network service for more than an hour for no reason, check immediately. 2. **Unexpected Call:** You might receive a call saying "We are testing your line, please press 1." This is a check to see if your number is ready for the swap. Do not follow such instructions from anyone, just Hang up. 3. Check you email for any unsuspecting emails stating any changes in your accounts or password resets etc.
Steps to Remediate	1. **Immediate Check:** If service is lost, immediately call your telecom provider's customer care from a *different* phone (a family member's) and ask them to verify if a SIM swap was requested. 2. **Block:** If a swap is confirmed, ask them to **block your SIM immediately** and simultaneously call your bank to freeze all accounts linked to that number.
Remember	1. Never lose service for more than 1 hour without confirming with your provider.

	2. Use strong passwords for your email, biometric mobile lock or a strong 6 digit pin not 123456 or 654321 or all zero etc. 3. Any identification documents you submit, mention the purpose and date on the document.
Reporting	**Whom:** Telecom Provider & Bank Fraud Department.

Threat #12: The "Customer Service" Imposter Call

The classic trap that relies on you having a real problem.

- **Targets:** People searching for customer care numbers online for getting support from Amazon, Bank, Electricity or delivery oof medicines or alcohol from nearby areas.
- **Medium of Attack:** Spoofed phone numbers and fake websites.
- **Objective:** To get remote control access to your phone or trick you into a payment by sending you a fake link or QR code for payment.

The Scenario:

You search on Google for "SBI Credit Card Customer Care." The very first result (a paid advertisement) shows a number. You call it.

The "Executive" is very helpful. They say: "Your problem requires a simple fix. Please install the AnyDesk app and give me the 9-digit code so I can fix the issue remotely." Or for orders , they provide you a payment link or QR code.

Phase	Details
Steps to Identify	1. **The Website:** The number you called came from a suspicious website that was NOT the official bank or delivery or support web site. 2. **Remote Access Demand:** Real customer service will **never** ask you to install AnyDesk or TeamViewer on your phone for a simple query. 3. **Payment Link:** If they ask you to pay a ₹1 fee to "verify" the fix, that payment is used to steal your UPI PIN.
Steps to Remediate	1. **Never Trust Google Search:** Always go to the **official** bank/company website and look for the "Contact Us" section. The real number is always there. 2. **Do Not Install:** Never install remote access apps for a stranger. If you did, uninstall it immediately and change all passwords. **3. Never pay to unknown websites or QR codes :** Never install remote access apps for a stranger. If you did, uninstall it immediately and change all passwords.
Remember	**Rule:** Only use customer care numbers found on your physical card, official statements, or the official app.
Reporting	**Whom:** Google/ Microsoft Bing etc (Report the misleading ad) & Cyber Crime (1930).

Threat #13: The Malicious Text Message (Smishing)

A text message that tricks you into giving up credentials.

- **Targets:** Smartphone users.
- **Medium of Attack:** SMS (Smishing) with a fake link.
- **Objective:** To direct you to a phishing website to steal passwords.

The Scenario:

You get a text message: "Your Amazon order is arriving today. If you need to change the delivery time, click here: http://amazon-track-delivery.com"

You click the link, and it takes you to a website that looks exactly like Amazon and asks you to log in. You enter your password, and the scammer now has your Amazon password (and likely your bank password if you reuse it).

Phase	Details
Steps to Identify	1. **Shortened Links:** The URL in the text is a shortened link or a slightly misspelled official name (e.g., amazon-track.net instead of amazon.in). 2. **The Credential Demand:** The link takes you to a login page, asking for your username and password, even when you didn't need to log in for a simple tracking update.
Steps to Remediate	1. **Check Official App:** If you get a tracking message, ignore the link. Open the **official** Amazon/Flipkart app on your phone to check your order status. 2. **Long Press:** On Android phones, you can often "long press" the link to see the full, real address before clicking. If it looks suspicious, report it and than delete it.
Remember	**Rule:** Never trust a link in an unexpected text message. Always use the company's official app to verify details.
Reporting	**Whom:** Forward SMS to **1909** (Telecom Phishing Reporting).

Threat #14: WhatsApp "Lost Phone" Scam

A simple, high-impact emotional trick to steal your chats and identity.

- **Targets:** WhatsApp users with family and friend contacts.
- **Medium of Attack:** WhatsApp message from an unknown number.
- **Objective:** To get you to send them the six-digit WhatsApp registration code, thereby taking over your account.

The Scenario:

You receive a WhatsApp message from a number you don't recognize, using your friend/family member's photo. It says: "Hi, I lost my phone, this is my new number. Can you do me a huge favor? WhatsApp is sending a 6-digit verification code to your number by mistake; please send it to me immediately."

If you send the code, the scammer instantly registers your WhatsApp account on their device, locking you out and gaining access to all your personal chats and contacts.

Phase	Details
Steps to Identify	1. **The Lie:** WhatsApp never sends a verification code to a random friend's phone "by mistake." 2. **The Code:** The code is the **key** to your account. The message says: *"Do not share this code with anyone."* 3. **The Urgency:** They demand the code within seconds, before you can think.
Steps to Remediate	1. **Call & Verify:** Immediately call your friend/family member on their **old, known** number to verify they actually lost their phone. 2. **Set PIN:** Go to WhatsApp Settings > Account > **Two-Step Verification** and set a 6-digit PIN. This is the **only** thing that will protect your account if a scammer gets the registration code or OTP. Don't share this with anyone and don't keep it like 123456 or something easy
Remember	**Rule:** The 6-digit code is the key to your digital home. Never share it with anyone, not even your closest relative.
Reporting	**Whom:** Report and Block the new number on WhatsApp.

Threat #15: Wi-Fi Spoofing – Free Unlimited Internet Scam

A simple, high-impact attack to steal your email account , financial information and identity using a fake WiFi connection.

- **Targets:** Anyone using public WiFi in places like cafes, airports, malls, hotels, libraries, trains or bus stations. People attracted by SSIDs like "Free WiFi", "Free Unlimited Internet", "High Speed Airport WiFi", or misspelled versions of the venue's real WiFi.
- **Medium of Attack:** Fake / rogue WiFi hotspot (technically called as "evil twin") created using a phone, laptop, or portable router with a tempting SSID such as "Free High Speed Internet" or "Airport Free WiFi".
- **Objective:** To get you to hooked to fake WiFi, intercept the traffic, inject fake login pages to capture passwords or credit card data

The Scenario:

You are at an airport / café where genuine WIFI is slow or keeps disconnecting. You notice another network with a stronger signal and names like "Free High Speed Internet", "Airport_Free_5G", or "Café_WiFi_Free_Unlimited". It does not ask for the usual password or captive-portal page used by the venue, or it shows a basic login page that asks for email, phone, or even card details "for verification". Once connected, your browsing appears normal but the attacker is silently capturing everything you type, including OTPs and card details during payments.

Phase	Details
Steps to Identify	1. **Valiate with staff** for exact WiFi name and password instead of guessing from the list; avoid networks that just say “Free WiFi” etc. **2. Be suspicious** if there are two very similar SSIDs (e.g., “Cafe_WiFi” and “Cafe-WiFi-Free”) or if the “free” network has a much stronger signal than the official one. **3. Check the browser address bar:** if banking, shopping, or email pages are not using https (no padlock) or show certificate warnings, disconnect immediately. **4. Unusual behaviour –** If after connecting, you observe unusual pop-ups, forced redirects to login pages, or requests to “update” plugins or install apps, disconnect.
Steps to Remediate	1 Immediately disconnect WiFi and forget that network on the device so it does not auto-reconnect later. 2. If you entered any passwords while on the suspicious WiFi, change those passwords quickly using a trusted connection (mobile data or known safe WiFi) and enable multi-factor authentication. 3. If you entered card or banking details, contact the bank / card provider, block the card if needed, and monitor transactions or enable alerts.
Remember	1. Avoid using public / free WiFi for any banking, UPI, wallet, trading, or shopping transactions; use mobile data or a trusted network instead. 2. Turn off auto-connect to open networks on phones/laptops so the device does not silently join a rogue hotspot. 3. Use VPN if you must connect to a public WiFi/Free WiFi.
Reporting	**Whom:** Report to local staff and the venue incharge.

Chapter 4: The Emotional Manipulators (Heart & Greed)

"Hackers know that when your heart is beating fast—either from love, fear, or excitement—your brain stops thinking. They don't hack computers; they hack human feelings."

In this chapter, we discuss scams where the criminal acts as a friend, a lover, or a scared relative. These are psychological attacks designed to make you act quickly without verifying.

Threat #16: Romance Scams (The "Military Doctor" Trap)

Love is blind, Sex is exciting and scammers count on it.

- **Targets:** Widows/Widowers, Divorcees, Seniors on Facebook/Matrimony sites.
- **Medium of Attack:** Facebook, Instagram, Matrimonial Apps (Shaadi/Jeevansathi), WhatsApp.
- **Objective:** To drain your life savings by promising a future life together.

The Scenario:

You meet someone online. He claims to be a Doctor in the UK or a US Army Officer. You chat for weeks. He proposes marriage. Suddenly, he sends a message: "I am coming to India to marry you, but I have been stopped at Customs/Airport because I am carrying Gold/Foreign Currency. Please pay the tax of ₹50,000 to release me." OR "I am coming to meet you however I am unable to book the ticket using international card, Pls share the card details so that I can book the tickets."

Phase	Details
Steps to Identify	1. **The Job:** They almost always work "abroad" or in dangerous places (Army, Oil Rig, Ship) where they "cannot video call easily." 2. **The Emergency:** The request for money is always a sudden crisis (Customs, Hospital, ticket booking issues, frozen bank account). 3. **The Account:** They are supposedly foreign, but they ask you to deposit money into a **local Indian bank account** belonging to a stranger or ask for account details or credit card details for ticket booking.
Steps to Remediate	1. **The "Video Test":** Demand a high-quality video call where they do a specific action (e.g., "scratch your head" or move your head right and left in fast motion"). If the video call is deep fake, they will be caught. If they make excuses, block them. 2. **No Money:** Never send money to someone you haven't met in person, no matter how much you "love" them or are attached to them. 3. **Reverse Image Search:** Upload their photo to Google Images. You will likely find the photo belongs to a real (innocent) person who is not even aware..
Remember	**Rule:** True love does not ask for money transfer fees. If "Customs" holds them, let them handle it.
Reporting	**Whom:** The Social Media Platform from where you became friends & Cyber Crime.

Threat #17: The "Grandchild in Trouble" (AI Voice Scam)

The most terrifying scam for parents/grandparents.

- **Targets:** Senior Citizens, Parents with children studying abroad/in other cities.
- **Medium of Attack:** Landline or Mobile Call sometimes with lot of background noise to mimic an emergency situation.
- **Objective:** Immediate panic transfer of funds.

The Scenario:

Your phone rings. You hear your grandson/son's voice. He is crying.

"Grandpa, please help me. I was in an accident... I hit a lady... The police are here... Here, talk to my lawyer."

A "Lawyer" then takes the phone and says: "He is in deep trouble. Transfer ₹1 Lakh for bail immediately or he goes to jail."

The other scenario can be a fake kidnap call mentioning that we have kidnapped your son or grand daughter while he/she is playing or on a tour.

Phase	Details
Steps to Identify	1. **Emotional Pressure:** They won't let you think. Crying + Police Sirens in the background. 2. **Secrecy:** *"Don't tell Mom/Dad, they will be angry. Just help me."* 3. **The Transfer:** The "Lawyer" asks for money via UPI/Transfer, not to a court, but to a personal account.
Steps to Remediate	1. **Hang Up & Verify:** Hang up. Call your grandchild's **original** number immediately. 2. **Ask a Personal Question:** Ask something AI doesn't know. "What did I cook for you last Sunday?" 3. **The Family Password:** Create a secret "Safe Word" today (e.g., "Purple Mango"). Tell your family: *"If you are ever in real trouble, you must say this word."*
Remember	**Rule: Create a Family Safe Word today. This is the single best defense against AI voice scams.**
Reporting	**Whom:** 1930 (Cyber Crime).

Threat #18: Sextortion (The Video Call Blackmail)

A moment of curiosity leading to months of shame.

- **Targets:** Men (mostly), Teenagers or seniors.
- **Medium of Attack:** WhatsApp Video Call / Facebook Messenger.
- **Objective:** Blackmail and extortion.

The Scenario:

You get a video call from a random number. You answer out of curiosity.

On the screen, you see an attractive woman stripping or behaving inappropriately. You stare in shock for 10 seconds.

The Trap: The video is a pre-recorded clip. You are the one being recorded. They capture your face watching the video.

Minutes later, you get a message: "I have recorded you watching dirty videos. Pay me ₹50,000 or I will send this video to your wife, boss, and Facebook friends list."

Phase	Details
Steps to Identify	1. **Unknown Video Call:** Random video calls from strangers are almost always this trap. 2. **The Threat:** They send you a screenshot of your friends list (which they stole from Facebook) to prove they can ruin your reputation.
Steps to Remediate	1. **DO NOT PAY:** This is the most important rule. If you pay once, they will ask again tomorrow. 2. **Block & Ignore:** Block the number. Deactivate your social media for a week. They usually move on to the next victim if you don't respond. 3. **Lock Down Privacy:** Ensure your Facebook friends list is set to "Only Me." 4. Inform via a Socia Media post that a Deep Fake video of you is circulating, don't trust the video.
Remember	**Rule:** Put a sticker over your selfie camera when not in use. **Never answer video calls from unknown numbers.**
Reporting	**Whom:** Cyber Crime (1930). This is a serious offense.

Threat #19: Part-time Job / "Task" Scams

The trap of "Easy Money."

- **Targets:** Housewives, Unemployed Youth, Students.
- **Medium of Attack:** WhatsApp / Telegram.
- **Objective:** To steal your savings under the guise of "investing" in a job.

The Scenario:

You get a message: "Work from home! Earn ₹5,000/day just by liking YouTube videos."

They pay you ₹150 for the first few tasks. Trust is built.

Then comes the "Prepaid Task": "To get higher paying tasks (₹10,000), you must invest ₹2,000 as a security deposit. You will get back ₹2,800."

You pay and You get the money back. Then they ask for ₹50,000. You pay... and they disappear.

Phase	Details
Steps to Identify	1. **Pay to Earn:** Real jobs **pay you**. You never have to pay money (deposit/investment) to get a salary. 2. **Telegram Shift:** They usually move the conversation from WhatsApp to Telegram for the "big tasks." 3. **Too Good to Be True:** Liking a video takes 1 second. Why would anyone pay ₹5,000 for that?
Steps to Remediate	1. **Stop Paying:** If you have paid, stop immediately. Do not pay "taxes" or "withdrawal fees" to get your money back. 2. **Exit:** Block the group/contact.
Remember	**Rule:** If a job asks you to pay money to start working, it is a scam. 100% of the time.
Reporting	**Whom:** Telegram (Report Channel) & Cyber Crime (1930).

Threat #20: Lottery & Inheritance Scams

The "Nigerian Prince" scam, updated for 2025.

- **Targets:** Everyone (via Email/Letter).
- **Medium of Attack:** Email, WhatsApp, Physical Post.
- **Objective:** Advance Fee Fraud.

The Scenario:

You receive an email or a WhatsApp image: "Congratulations! Your mobile number has won £1 Million in the Coca-Cola Lottery." OR "I am the bank manager for a deceased billionaire who shares your last name. I need your help to move his $50 Million fund. We will split it 50/50."

Phase	Details
Steps to Identify	. **Did you buy a ticket?:** You cannot win a lottery you did not enter. 2. **Processing Fee:** They will say the money is ready, but you must pay a "Customs Duty" or "Transfer Fee" of ₹25,000 to release it. 3. **Poor Grammar:** Official letters from Coca-Cola or BMW do not have spelling mistakes or come from Gmail addresses.
Steps to Remediate	1. **Delete:** Do not reply. Replying confirms your email/number is active. 2. **Verify:** Visit the official website of the company mentioned. They usually have a "Fraud Alert" page warning about these exact scams. Also inform them via contact us link.
Remember	**Rule:** You have to play to win. If you didn't buy a ticket, it's a lie. Real prizes deduct tax from the winnings; they never ask you to pay upfront.
Reporting	**Whom:** Email Provider (Mark as Phishing).

Chapter 5: Technical Hygiene & Future Threats

"Technology is a great servant but a terrible master. We must learn the simple habits that keep our devices—and our money—safe."

This chapter covers the basic habits which can prevent 90% of technical attacks, alongside the new threats that are evolving through Artificial Intelligence including DeepFake based scams.

Threat #21: Deepfakes (AI Video/Audio)- The Technical View

Using Artificial Intelligence to make lies believable.

- **Targets:** Unsuspecting users who are generally active on social networks.
- **Medium of Attack:** Social Media (Voice notes, Reels, YouTube).
- **Objective:** Identity theft and financial fraud (impersonation), misinformation and disinformation.

The Scenario:

A scammer uses an AI program to clone the voice of your boss or a bank manager from a short public video. They call you, and the voice sounds perfectly real, telling you to transfer funds for an "urgent deal." Even Deep Fake Video calls have been used for asking sub-ordinates or family members to transfer money. Attackers have even cloned “Mukesh Ambani” and “Smt Seetharaman, Finance Minister” for posting advertisements promising huge returns with trading.

Phase	Details
Steps to Identify	1. **Lack of Interaction:** The face/mouth in a video deepfake may not sync perfectly with the voice. 2. **Robotic Sound:** The AI voice sounds too smooth or lacks the natural "hmm" and "uhh" pauses of real speech. 3. **The Urgent Ask:** The request is always for immediate money transfer and always bypasses normal communication channels.
Steps to Remediate	1. **Limit Sharing:** Set social media posts (especially those with your voice) to "Friends Only" or "Private." 2. **The Safe Word:** Use your family password (as defined in Chapter 4) to confirm the identity of the caller. 3. **Call Back:** Hang up and call the person back on their *known* mobile number.
Remember	**Rule:** If you hear the voice of a loved one demanding money, **never** transfer funds until you have called them back on their original number and used the safe word.
Reporting	**Whom:** Cyber Crime (1930). Also report fake videos /posts depicting credible Public figures to the social media platform. Generally each platform has an option to raise a complaint against the advertisements and social media posts.

Threat #22: Juice Jacking

The risk of public mobile charging.

- **Targets:** Travelers, people using airports, railway stations, coffee shops.
- **Medium of Attack:** Public USB charging stations.
- **Objective:** Stealing personal data, passwords, or installing malware.

The Scenario:

You plug your low-battery phone into a public USB charging port at the railway station. Unknown to you, a hacker has modified the port to also act as a data port, stealing photos and passwords from your phone while it charges.

Phase	Details
Steps to Identify	**USB Port:** The charging cable at a public station is not just carrying power; it can carry **data** (like transferring photos to your computer). There is no way to identify if a usb charging point is being used for data transfer during charging.
Steps to Remediate	1. Use a USB data blocker ("USB condom") or a charge-only cable when using any public or untrusted USB port , these physically disconnect the data pins and only pass power, so even a malicious kiosk cannot start data transfer. 2. Prefer your own wall charger plugged into an AC socket instead of plugging directly into unknown USB ports at public places like airports, malls etc. 3. Keep the phone's USB default set to "Charging only" and do not approve any "Allow data access?" when connecting to public charging points. 4. Avoid unlocking the phone while it is plugged into an unknown USB port.
Remember	**Rule:** If you need to charge your phone, only use your charger and a **wall socket**. If you need internet, use your own mobile data (hotspot).
Reporting	**Whom:** The establishment manager (Coffee shop/Airport).

Threat #23: Weak Passwords & Reuse

How one little mistake can unlock your whole life.

- **Targets:** Everyone with online accounts.
- **Medium of Attack:** Hacked websites and databases.
- **Objective:** Taking over multiple accounts using one stolen password if users use the same password for multiple sites (**Credential Stuffing**).

The Scenario:

You use the password Akash1983 for a small online shopping site. That site gets hacked, and the hacker steals your password. They then use Akash1983 to try and log into your Gmail, Facebook, and Bank accounts. If you reused it, they are instantly in.

Phase	Details
Steps to Identify	1. **Generic Passwords:** Using simple names (sunita123), dates (1960india), or word patterns (password1). These are cracked instantly. 2. **Account Lockouts:** You notice your Gmail or Facebook is suddenly locked, even though you didn't touch it.
Steps to Remediate	1. **Long Passwords:** Create passphrases that are 12+ characters long (e.g., BlueCurtains@MyHouseT3). 2. **Password Manager:** Use password managers like Zoho Vault , 1Pass etc to create and save unique passwords for every site. 3. **2FA/OTP: Crucial:** Turn on **Two-Factor Authentication (2FA)** for your Gmail, Hotmail, and other emails , WhatsApp, Social media and all bank accounts. This means even if a hacker has the password, they still need the mobile OTP.
Remember	**Rule:** Treat every password like a underwear —never share it, and change it often. **Activate 2FA everywhere.**
Reporting	**Whom:** Account provider (Google/Microsoft/Email service providers).

Threat #24: Social Media Cloning

Your face, your name, asking your friends for help.

- **Targets:** People with public social media profiles – who have not turned on the private or limited to friends list option.
- **Medium of Attack:** Facebook, Instagram, WhatsApp, X (formerly Twitter).
- **Objective:** To borrow money from your friends/family by impersonating you.

The Scenario:

A criminal copies your profile picture and name and creates a new, fake profile. They then send friend requests to all your family. They message your brother: "Hi, I lost my phone, and I need ₹20,000 immediately. Can you UPI me?"

Phase	Details
Steps to Identify	1. **Second Profile:** A friend receives a second friend request from you. 2. **The Story:** The cloned profile immediately messages your friends saying, *"My bank account is blocked, I lost my phone, or I need ₹10,000 for an emergency."* 3. **Low Activity:** The fake profile has your picture but zero friends or posts.
Steps to Remediate	1. **Privacy Settings:** Set your Friends List to **"Only Me"** so scammers cannot see your connections to target them. 2. **Warn Friends:** If you are cloned, immediately post on your *real* profile: *"Warning: I am being impersonated. DO NOT accept any second friend requests or send money."*
Remember	**Rule:** If a friend asks for money via messenger, call them on their *known* phone number to verify before sending a single rupee.
Reporting	**Whom:** The Social Media Platform (Report the fake account).

Threat #25: Malicious Email Attachments – No. 1 Attack Vector

The risk lurking in your email inbox – Email is also the top priority asset for hackers to attack.

- **Targets:** Anyone with an email accounts - virtually every single person using android, apple or WhatsApp – all these email ID registration.
- **Medium of Attack:** Email attachments (PDF, Excel, Zip files), malicious links.
- **Objective:** Installing Ransomware (locking your files and demanding money).

The Scenario:

You open an unexpected email from "The Bank" with a PDF attachment titled "Final Statement." The PDF contains a virus that locks all your photos, documents, and files. A message pops up: "Pay us ₹50,000 in Bitcoin to unlock your computer."

Phase	Details
Steps to Identify	1. **Unexpected Files:** You receive an invoice, order receipt, or a "bank statement" you didn't expect. 2. **The Type:** Files ending in .exe (executable), .zip, or a suspicious .pdf or .xlsx that forces you to "Enable Content" are dangerous.
Steps to Remediate	1. **Do Not Open:** If you don't know the sender, delete the email immediately. 2. **Enable Backup:** The best protection against Ransomware is a strong backup. Use Google Drive, Apple iCloud, or an external hard drive to copy all important photos and files regularly. 3. **Anti-virus Scan :** Use a good licensed anti-virus with anti-ransomware protection on your computer.
Remember	**Golden Rule:** Never pay , paying does not guarantee that you will get back your files. **Golden Habit:** Always backup your important files. If your computer gets locked by a virus, you can wipe it clean, reinstall the system, and restore your files from the backup. The hacker loses.
Reporting	**Whom:** Your Email Provider (Mark as Spam/Phishing).

Difference between "Beware to Being Aware" with the 3 Simple Habits That Save Your Life

Cybersecurity is not about installing complex software; it's about **making smart choices** based on three easy habits:

Habit 1: STOP

- **Pause Before You Click:** Whenever you feel a rush (fear, excitement, urgency), **STOP**. A real bank, police officer, or relative will never force you to rush an important financial decision.
- **Never Pay Upfront:** If someone promises you money (prize, job, inheritance) or marriage, but asks you to pay a fee or pay for customs or for travel first, **STOP**. It is a scam.

Habit 2: LOOK

- **Look at the Details:** Look at the sender's email address (is it **realbank.com** or **realbank-service.net**?). Look at the payment button (does it say **PAY** or **RECEIVE**?).
- **Look for the PIN:** If you are asked to enter your UPI PIN, ATM PIN, or Credit Card OTP, **LOOK** at the screen. You are about to give money away.

Habit 3: VERIFY

- **Verify on a Second Channel:** If your friend asks for money on WhatsApp, **VERIFY** by calling them on their usual phone number or check with their family members.
- **Verify with the Source:** If you get a bank warning via SMS, **VERIFY** by opening your official banking app directly. Do not click the link in the message.
- **The Safe Word: VERIFY** the identity of loved ones using your family safe word.

Your Final Emergency Kit

Service	What It Does	Contact/Website
Cyber Crime Helpline	To report financial fraud immediately.	Call **1930** (24/7)
National Cyber Reporting	For detailed complaints (Sextortion, ID Theft).	**cybercrime.gov.in**
Bank Block	To immediately freeze your card/account.	Call your bank's toll-free number.
Mobile Provider	To report SIM Swap or stolen phones.	Visit your nearest provider store.

You are the Lock on the Door to Your Finances and Privacy. Keep it Strong!!

@Cyber24x7